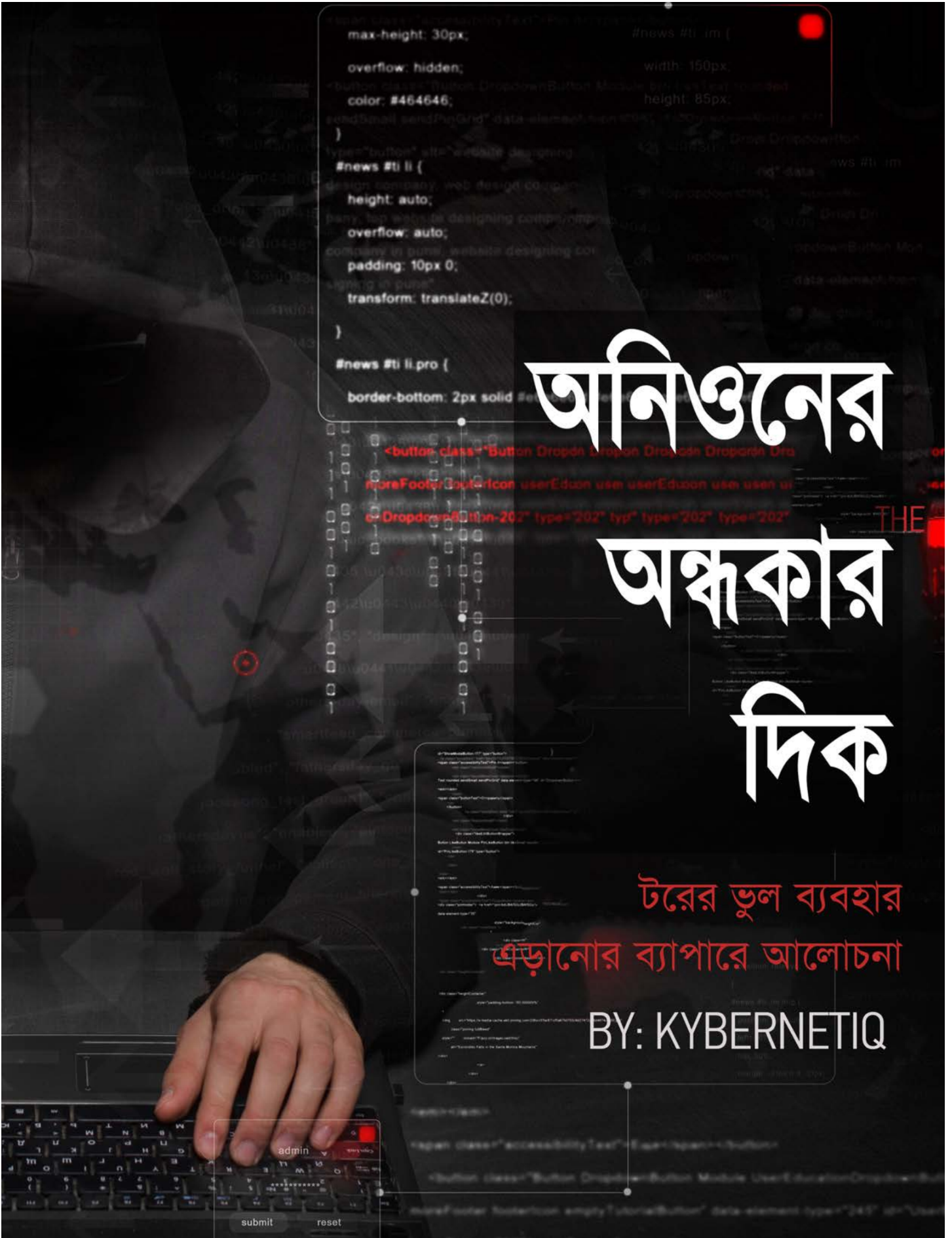


অনিওনের অন্ধকার দিক

টরের ভুল ব্যবহার
এড়ানোর ব্যাপারে আলোচনা

BY: KYBERNETIQ



Zero-Day-Exploits, চিহ্নিত Malware আক্রমণ, এবং খারাপ Exit-Nodes, টর ব্যবহারকারীর জন্য অত্যন্ত বিপজ্জনক সমস্যাগুলোর অন্তর্ভুক্ত হয়ে থাকে।

টর প্রজেক্টের দ্বারা উদ্ভাবিত টর ব্রাউজার আমাদের প্রতিরক্ষার সহায়ক হাতিয়ারগুলোর মধ্যে সবচেয়ে গুরুত্বপূর্ণ কৌশলের একটি।

এটি আমাদের অবস্থান লুকিয়ে ও অগ্ন্যত করে রাখে এবং আমাদের নজরদারী হতে অদৃশ্য করে রাখে; ফায়ারওয়াল ভেদ করে এবং বৈধ ইন্টারনেটের একটি প্রবেশপথ হিসেবে কাজ করে।

যাই হোক, এটাকে অবহেলার সাথে ব্যবহার আপনাকে দৃষ্টিগোচর করতে পারে এবং ইন্টেলিজেন্স সংস্থাগুলোর অনলাইনে আক্রমণের প্রতি অসুরত করে তুলতে পারে। অন্যান্য যেকোন সফটওয়্যার প্যাকেজের মতো টর এরও কিছু দুর্বলতা আছে।

টর ব্যবহারকারীর পরিচিতি বের করার জন্য বিভিন্ন কৌশল আছে। কিন্তু এর প্রোগ্রামারদের দ্বারা এর দুর্বলতাগুলোর বেশীরভাগই চিহ্নিত ও সারানো হয়ে গেছে, তাই এই হামলাগুলো আর কার্যকরী নয়।

নিশ্চিতভাবেই এমন কিছু সিক্রেট সার্ভিস এবং কোম্পানি আছে যারা সিকিউরিটি ভেদ করতে পারদর্শী এবং আপনাকে আক্রমণ করতে দিনরাত সক্রিয়ভাবে কাজ করে যায়।

সাম্প্রতিকভাবে প্রকাশ পায় যে, টর প্রজেক্টের একজন প্রোগ্রামার এফবিআইয়ের হয়ে কাজ করছিল এবং সে তাদের সাথে মেলিসিয়াস সফটওয়্যারে কাজ করছিল। ইটালিয়ান কোম্পানি হ্যাকিং টিমও Tails অপারেটিং সিস্টেমে হামলা করার জন্য কাজ করেছিল।

টর ব্যবহার করার সময় সবচেয়ে মৌলিক সমস্যাগুলোর মধ্যে একটি হচ্ছে এক্সিট নোডগুলো যা অপসারণ করা সোজা নয়।

“এমনকি যখন আপনি কিছুই করছেন না, তখনো নজরদারিতে আছেন এবং তথ্য সংগ্রহ করা হচ্ছে

এডওয়াড মোডেন

এটি শুধু টর নেটওয়ার্কের সমস্যা নয় বরং এটা আমাদের সাধারণ ইন্টারনেট ব্যবহারেরই একটা সমস্যা।

এর কারন হল, আপনি কোন দেশে বাস করেন তার উপর ভিত্তি করে আপনার প্রোভাইডার আপনার নেটওয়ার্কের ভেতর দিয়ে যাওয়া সকল তথ্য সংরক্ষণ করে।

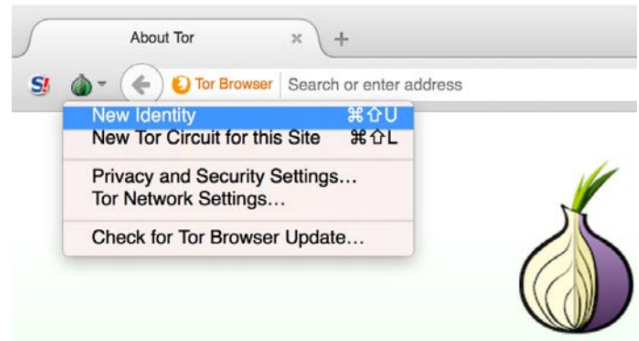
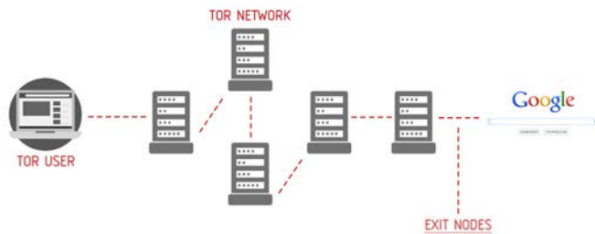
প্রকৃতপক্ষে, এন্ট্রি গার্ড টর রিলের প্রতি কানেকশন এনক্রিপ্ট করে রাখে এবং পালক্রমে এক্সিট নোডের কাছেও প্যাকেজগুলোকে এনক্রিপ্ট করে রাখে, কিন্তু আপনার ডাটাগুলো এক্সিট নোড হতে বের হয়ে যাবার পর আপনার প্রবেশকৃত ওয়েবসাইট দ্বারা পরীক্ষণের জন্য আবার খোলা হয়।

যদিও আপনার আইপি এড্রেসটি মাস্ক করা হয়েছে, যে ব্যক্তিটি এক্সিট নোড এবং আপনার প্রবেশকৃত ওয়েবসাইটের মধ্যকার ট্রাফিক নিয়ন্ত্রণ করে সেই এর মধ্যে দিয়ে যাওয়া সকল ট্রাফিক নিয়ন্ত্রণ করে। আক্রমণকারী এখন আপনার নেটওয়ার্কের উপর প্রয়োগকৃত এনক্রিপশনগুলো পরিবর্তন করতে, সরাতে এমনকি পরোক্ষভাবে বন্ধও করে দিতে পারে।

আপনি হয়ত খেয়াল করেছেন যে, Pidgin ম্যাসেনজার মাঝেমাঝে একটি সার্টিফিকেট প্রব্লেমের প্রতি নির্দেশ করে এবং আপনি কোন এনক্রিপ্টেড ওয়েবসাইটে ঢুকলেও এই সার্টিফিকেট প্রব্লেমেটি দেখায়। এই কানেকশনগুলো Corrupted এবং আপনি এই কানেকশনগুলো Accept করলে আক্রমণকারী আপনার সংবেদনশীল ডাটাগুলো পাবে এবং এবং তা এক্সেস করতে পারবে, যদিও এই কানেকশনগুলো এনক্রিপ্টেড। আক্রমণকারী এই সার্টিফিকেট তৈরী করে এবং এই কারনে সে এটার কী জানে। সেই প্যাকেজগুলোকে স্থানান্তর করে এবং ইচ্ছামত এগুলোকে তদারকি, পরিবর্তন বা ডিলিটও করতে পারে।

যদি আপনি সার্টিফিকেট ওয়ার্নিং এর মুখোমুখি হন তবে আপনার টর নেটওয়ার্কের কানেকশনটি রিস্টার্ট করা উচিত।

আপনি এটি আপনার টর ব্রাউজারের ওনিয়ন বাটনে ক্লিক করে "New Identity" তে ক্লিক করে করতে পারেন। একারণে আপনার যদি সম্ভব হয় তাহলে সবসময়ই এনক্রিপ্টেড কানেকশনে জোর দেয়া উচিত।



- এখানে নিরাপত্তামূলক সতর্কতার জন্য কিছু উপদেশ দেওয়া হল:
- টর ব্রাউজার বাভেল, টর ম্যাসেকার এবং Tails তাদের অফিসিয়াল ওয়েবসাইট থেকে ডাউনলোড করুন, এছাড়াও Cryptographic Signature ও Hash ভ্যালুগুলোও পরীক্ষা করে দেখুন।
- আপনার টর ব্রাউজার বাভেল, টর ম্যাসেকার, Tails এবং এগুলোর সকল প্লাগিনগুলো যেন সবসময় আপডেটেড থাকে সেদিকে খেয়াল রাখুন।
- সবসময় ইংলিশকে ডিস্ট ভাষা হিসেবে ব্যবহার করুন।
- ব্রাউজারের উইন্ডোটি ম্যাক্সিমাইজ করবেন না।
- আপনার সাধারণ ব্রাউজারটিতে টরকে প্রক্সি হিসেবে ব্যবহার করবেন না।
- আপনার টর ব্রাউজারের সেফটি লেভেলকে "upper medium" বা "high" করে রাখুন।
- যখনই সম্ভব হয় "JavaScript" এর পরিবর্তে "NoScript" ব্যবহার করুন।
- Adobe Flash Player ও অন্যান্য বাড়তি এড-অন ইনস্টল করবেন না।
- এমন কোনো SSL-certificates এক্সেপ্ট করবেন না যার উৎস আপনি জানেন না।
- যখনই সম্ভব হয় এন্ট-ট্র-এন্ট এনক্রিপ্টেড কানেকশন ব্যবহার করুন।
- ইন্টারনেটে কানেক্টেড থাকা অবস্থায় আপনার কোন পিডিএফ, ফোন্টার বা ফাইল খোলা উচিত নয়, যদি সম্ভব হয় তবে এগুলো কোন ভার্চুয়াল উইন্ডোতে (যেমন: লিনাক্স) ওপেন করুন।
- অপ্রয়োজনীয় এবং পুরোনো প্লাগিন ব্যবহার বর্জন করুন।
- আপনার ব্যক্তিগত পরিচিতি হতে আপনার জিহাদী কাজগুলো বা এমন কাজকর্ম ও ডাটা যা পরবর্তীতে আপনাকে বা অন্য মুসলিমকে সনাক্ত করতে পারবে তা আলাদা রাখুন।
- আপনার সাধারণ ইন্টারনেট ব্রাউজিং এর সময়কার পরিচয় ও পাসওয়ার্ডগুলো ডার্কনেটে ব্রাউজিং এ ব্যবহার করবেন না।
- আপনার ডার্কনেটের আইডিগুলোতে সাধারণ কানেকশন ব্যবহার করার সময় টর ছাড়া লগ-ইন করবেন না।



"আমাদের এটা ধরে নেওয়া উচিত যে, শত্রুরা এই ডিজিটাল যোগাযোগগুলো দেখতে পারে এবং

আমাদের এবং আমাদের ইলেক্ট্রনিকভাবে সেন্সব তথ্যই পাঠানো উচিত যা শত্রুরা পড়লে কোন ক্ষতি হবে না। এটা এনক্রিপ্টেড দেখে আমাদের এটায় ভরসা করা উচিত হবে না, কারন শত্রুরা সহজেই মুজাহিদ্দীনদের অঞ্চলের ট্রাফিক পর্যবেক্ষন করতে পারে।

কম্পিউটার সায়েন্স আমাদের সায়েন্স নয় আর আমরা এটার উদ্ভাবকও নই। আমার মতে গোপন তথ্য পাঠানোর জন্য এনক্রিপশনের উপর ভরসা করা অনেক ঝুঁকিপূর্ণ।

এনক্রিপশন সিস্টেম সাধারণ লোকদের সাথে কাজ করে যারা নন-স্পেশালিষ্ট, তাদের সাথে নয় যারা ইলেক্ট্রনিক যোগাযোগ ও ইন্টারনেট আবিষ্কার করেছে। সকল সংবেদনশীল তথ্য চিঠির মাধ্যমে পাঠানো উচিত।"

শায়খ উসামা বিন লাদিন রাহিমাহুল্লাহ

আগস্ট ৭, ২০১০

আভ্যন্তরীণ যোগাযোগ